JC891 U.S. PTO
09/21/00

09-22-00

A

Docket Number F-208
Pitney Bowes Inc.
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000
September 21, 2000

JC892 U.S. PTO
09/667845
09/21/00

BOX PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

Sir:

Transmitted herewith for filing is the patent application of

Inventor: Douglas A. Clark

For: TAMPER DETECTION SYSTEM FOR SECURING DATA

Enclosed are:

Nineteen (19) pages comprising the specification, claims, and abstract.

Two (2) sheets of drawing.

A Declaration and Power of Attorney.

An Information Disclosure Statement.

A Recordation of Assignment Request and an Assignment of the invention to Pitney Bowes Incorporated, 1 Elmcroft Road, Stamford, Connecticut 06926-0700.

Certificate of Mailing by Express Mail. The Express Mail label number is EE628583118US.

Fees calculated as follows:

Basic Fee							$ 690.00
Claims Fee	Number Filed		Number Extra		Rate		
Total Claims	24	- 20 =	4	X	$18.00	=	$ 72.00
Independent Claims	3	- 3 =	0	X	$78.00	=	$ 0.00
Multiple Dependent Claims					$260.00	=	$
					Total Filing Fee		$ 762.00

Please charge our Deposit Account Number **16-1885** in the amount of $ 762.00 for the filing fee.

The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Account Number **16-1885**.

A copy of this Transmittal Letter is enclosed for use in charging the Deposit Account.

Angelo N. Chaclas
Reg. No. 39,134
Attorney of Record
Telephone (203) 924-3844

09667845 092100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:	) Attorney Docket No.: F-208
Douglas A. Clark	) Group Art Unit:
Serial No.:	) Examiner:
Filed:	) Date: September 21, 2000

Title: TAMPER DETECTION SYSTEM FOR SECURING DATA

CERTIFICATE OF MAILING BY EXPRESS MAIL

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 CFR 1.10, I hereby certify that the attached nineteen (19) pages comprising the specification, claims, and abstract, two (2) sheets of drawings, Declaration and Power of Attorney, Recordation of Assignment, Assignment, and Information Disclosure Statements with attachments was deposited with the U.S. Postal Service for delivery by Express Mail on September 21, 2000. The number of the Express Mail mailing label is EE628583118US.

Respectfully submitted,

Angelo N. Chaclas
Reg. No. 39,134
Attorney of Record
Telephone (203) 924-3844

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000

TAMPER DETECTION SYSTEM FOR SECURING DATA

Field of the Invention

This invention relates generally to data protection systems. More particularly, in the preferred embodiments, this invention is directed to a tamper detection system for detecting unauthorized attempts to access an integrated circuit.

Background of the Invention

In many different industries, there is a need to protect data (information) from discovery. Oftentimes, the data is resident within the discrete electronic components of an integrated circuit. In turn, the integrated circuit may be incorporated into a printed circuit board, a smart card or other electronic device. The data itself may be of a wide variety depending upon the particular industry. As examples, the data may be used in: monetary transactions (debit card, postage metering, etc.) and controlled access systems (security badges). Furthermore, the data may be cryptographic keys, account balances, some combination of these or any other type of data that is to be protected.

Because of the risks of fraud and security breaches, there is a great deal of industry attention dedicated to securing the data from tampering and/or preventing access to the discrete components of the integrated circuit. Generally, such measures are directed to both physical security (epoxy enclosures, sealed devices) and electronic security, such as: encryption, data protection devices and the like. Although these techniques generally work well, they can be costly to develop, reduce to practice and implement into production.

Therefore, there is a need for a cost effective and efficient system for detecting unauthorized attempts to access an integrated circuit so as to prevent the data contained within or operation of the integrated circuit from being tampered with.

Summary of the Invention

In the most preferred embodiments, the present invention provides a tamper detection system that includes a trigger mechanism system and a detection circuit that operate in combination to protect an integrated circuit from attack. The detection circuit connects to the trigger mechanism system that is basically a protective mesh that consists of two separate loops of wire held in close proximity to each other and an optional ground layer. The mesh is such that any attempted penetration is highly likely to cause an open of either loop or a short of one loop to the other. The detection system recognizes shorts and opens in the mesh. The detection circuit is intended to be very simple in its operation in that it does not require a sophisticated stimulus and response set to operate. It is designed to be polled on a regular basis for indications of a change in its operation.

In accordance with the present invention, there is provided a tamper detection system for securing a protected integrated circuit from attack. The tamper detection system includes a power source, a trigger circuit and a detection circuit. The trigger circuit includes a plurality of resistors and a plurality of wire loops where the plurality of resistors include a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source. The plurality of wire loops include a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor. The first wire loop and the second wire loop are electrically isolated from each other but in overlapping physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit. The detection circuit is in operative communication with the trigger circuit and the protected integrated circuit. The detection circuit monitors an uninterrupted flow of current through the trigger circuit (normal condition), such that an interruption or change in the current flow in the trigger circuit (attack attempt) due to an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop causes the detection circuit to output a predetermined signal.

Therefore, it is now apparent that the present invention substantially overcomes the disadvantages associated with the prior art. Additional advantages of the invention will be set forth in the description that follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

Brief Description of the Drawings

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate presently preferred embodiments of the invention, and together with the general description given above and the detailed description of the preferred embodiments given below, serve to explain the principles of the invention. As shown throughout the drawings, like reference numerals designate like or corresponding parts.

Fig. 1 is a simplified diagrammatic representation of a tamper detection system in accordance with the present invention.

Fig. 2 is a cross section taken through the tamper detection system and an integrated circuit in accordance with the present invention.

Detailed Description of the Preferred Embodiments

Referring to Fig. 1, a tamper detection system 100 in combination with a protected integrated circuit 20 that it protects is shown. The tamper detection system 100 includes a trigger circuit 110 and a detection circuit 160. Generally, the trigger circuit 110 is shown to the left of the phantom line PL while the detection circuit 160 is shown to the right. It should be understood that the phantom line PL does not constitute part of the present invention, but is merely used to illustrate the geometric relationship between the trigger circuit 110 and the detection circuit 160. Those skilled in the art will recognize that the distinction between the elements that have been designated are part of the trigger circuit 110 and the detection circuit 160, respectively, is subject to interpretation. However, as a general rule, the elements that an intruder would initially come into contact with during a tamper attempt have been

designated as the trigger circuit 110 while the remaining portions have been designated as the detection circuit 160.

Generally, the trigger circuit 110 and the detection circuit 160 operate as follows. The trigger circuit 110 is basically a protective mesh that envelopes/encloses the integrated circuit 20 that is to be protected. For the sake of clarity, in Fig. 1, the protected integrated circuit 20 has been shown separate from the trigger circuit 110. However, from the discussion below, those skilled in the art will appreciate that the trigger circuit 20 is intended to fully envelope the integrated circuit 20. The detection circuit 160 operates as a switch that detects breaches (shorts, opens, or ground shorts) in the trigger circuit 110 and provides an appropriate signal to the integrated circuit 20. This allows the integrated circuit 20 to initiate an appropriate response (i.e., zeroization of data, such as: cryptographic keys; self destruction, etc.) before the intruder has gained access to the integrated circuit 20.

The trigger circuit 110 includes a first wire loop LOOP A (shown in solid line), a second wire loop LOOP B (shown in dotted line to distinguish from the first wire loop LOOP A for clarity) and a ground layer G, all of which may be integrated into a common substrate such as a flex strip that envelopes the integrated circuit 20. The first wire loop LOOP A and the second wire loop LOOP B are not in electrical contact with each other or the ground layer G. However, to form the protective mesh, they are in physical proximity (overlapping, adjacent, interleaved, etc.) to each other. This may be achieved by integrating the first wire loop LOOP A and the second wire loop LOOP B into any number of different geometric patterns. Any pattern that is likely to cause the first wire loop LOOP A and the second wire loop LOOP B to come into electrical contact with each other in response to a variety of invasive attack attempts (drilling, probing, etc.) may be employed. Similarly, the ground layer G may also be a wire loop integrated with the first wire loop LOOP A and the second wire loop LOOP B or, in the alternative, may be a separate membrane (shield, layer, etc.) of the common substrate.

The detection circuit 160 includes four resistors R1, R2, R3 and R4 and two transistors Q1 and Q2. The detection circuit 160 is supplied by a voltage source V_{source} (such as a battery or other suitable supply of power) and yields

an output voltage V_{output} signal at a designated node of the detection circuit 160 between an end of the forth resistor R4 opposite to the voltage source V_{source} and the second transistor Q2. Under normal operating conditions, three of the resistors are aligned in series. The first wire loop LOOP A is connected between a first resistor R1 and a second resistor R2 while the second wire loop LOOP B is connected between the second resistor R2 and a third resistor R3. Generally, the values of the resistors should be selected in accordance with an acceptable amount of current draw for the given application while achieving a robust level of noise tolerance for the draw for the given application. Preferably, the resistors in series R1, R2 and R3 should be of the same value and suitable large impedance so that the current draw is sufficiently low to conserve power. A first transistor Q1, of the PNP type, includes three terminals: an emitter $Q1_e$, a collector $Q1_c$ and a base $Q1_b$. The first transistor emitter $Q1_e$ and the first transistor base $Q1_b$ are connected on either side of the second resistor R2, respectively, to allow a bias voltage to develop drop across the second resistor R2 which in turn allows the first transistor Q1 to conduct current. A second transistor Q2, of the NPN type, also includes three terminals: an emitter $Q2_e$, a collector $Q2_c$ and a base $Q2_b$. The second transistor base $Q2_b$ is connected to the first transistor collector $Q2_c$ while the second transistor emitter $Q2_e$ is connected to ground. The fourth resistor R4 is in parallel with the series resistors R1, R2 and R3 and is connected between the voltage source V_{source} and the second transistor collector $Q2_c$. The output voltage V_{output} is developed at the junction of the fourth resistor R4 and the second transistor collector $Q2_c$.

Referring to Fig. 2 in view of Fig. 1, a cross section taken through the tamper detection system 100 and the protected circuit 20 is shown. Although Fig. 2 depicts the wire loops LOOP A and LOOP B external to the ground layer G, this has been represented this way for ease of illustration. In the most preferred embodiment, the integrated circuit 20 is surrounded by the interleaved mesh of the wire loops LOOP A and LOOP B and then encapsulated by the ground layer G. This arrangement adds an element of shielding to the entire assembly. Furthermore, the detection circuit 160 is incorporated into the protected circuit 20. Those skilled in the art will

recognize that any suitable substrate (not shown), such as a flex strip, may be employed to carry the ground layer G and the wire loops LOOP A and LOOP B. Additionally, further protective coatings, such as epoxy based potting materials, may also be employed in combination with the elements discussed above.

Referring to Figs. 1 and 2, the detection circuit 160 will assert its output when: (i) the wire loops LOOP A and LOOP B are shorted together; (ii) either of the wire loops LOOP A or LOOP B is broken; or (iii) either of the wire loops LOOP A or LOOP B is shorted to the ground layer G. It is anticipated that an attacker could not physically access the protected circuit 20 without causing one of these conditions to occur. Because the tamper detection system 100 does not: (i) send out a pulse and monitor the response, or (ii) rely on a processor; those skilled in the art will understand that the detection circuit 160 is passively operated.

During normal operation (no tampering), the wire loops LOOP A and LOOP B and the ground layer G all remain separate (electrically isolated) and intact. Thus, the three resistors R1, R2, and R3 are in series and drawing a nominal amount of current. The voltage drop created across the second resistor R2 allows bias current to flow through the first transistor Q1 from the first transistor emitter $Q1_e$ to the first transistor base $Q1_b$. This causes the first transistor Q1 to be switched on (biased into conduction) so that the first transistor collector $Q1_c$ supplies current to the second transistor base $Q2_b$. With the first transistor collector $Q1_c$ supplying current to the second transistor base $Q2_b$, the second transistor Q2 is turned on. This causes the second transistor collector $Q2_c$ to be held low. With the second transistor Q2 switched on, the output voltage V_{output} is held low, or at roughly 0.2V. As discussed above, the forth resistor R4 should be sized to minimize the amount of current needed and still be robust and noise immune. In response to a low output voltage V_{output}, the protected circuit 20 assumes normal operation and takes no protective measures.

If the wire loops LOOP A and LOOP B were to be shorted together, then the output voltage V_{output} goes high as the first transistor Q1 and the second transistor Q2 are turned off, allowing the output voltage V_{output} to go

high. Generally, this would result because of the following. The second resistor R2 would be shorted and the voltage across it would go to zero. This would not allow a bias voltage to develop from the first transistor emitter $Q1_e$ to the first transistor base $Q1_b$ to switch on the first transistor Q1. Thus, the first transistor is switched off (out of conduction - the first transistor collector $Q2_c$ goes low) and this in turn starves the second transistor Q2 of current and it too will be switched off. Here again, the second transistor Q2 is switched off because not of a lack of current flow from the second transistor base $Q2_b$ to the second transistor emitter $Q2_e$. With the second transistor Q2 switched off, the output voltage V_{output} rises to equal the voltage source V_{source} because their exists an "open" between the second transistor collector $Q2_c$ and the second transistor emitter $Q2_e$.

If the first wire loop LOOP A is broken, then the output voltage V_{output} goes high by equaling the voltage source V_{source}. Generally, this would result because of the following. The connection (first wire loop LOOP A) from the first resistor R1 to the second resistor R2 is opened. As a result, the voltage drop across the second resistor R2 and the third resistor R3 goes to zero as the current flow producing the drop has been interrupted. As described above, this switches off the first transistor Q1, starves the second transistor Q2, turning it off too, and causes the output voltage V_{output} to rise equal to the voltage source V_{source}.

Similarly, if the second wire loop LOOP B is broken, then the output voltage V_{output} goes high by equaling the voltage source V_{source}. Generally, this would result because of the following. The connection from the second resistor R2 to the third resistor R3 is opened. As a result, the voltage drop across the first resistor R1, the second resistor R2 and the third resistor R3 goes to zero as the current flow producing the drop has been interrupted. As the voltage across the second resistor R2 goes to zero, with the removal of the current source to the first transistor Q1, the first transistor Q1 is switched off. Here again, this starves the second transistor Q2 of bias current and it switches off. However, the node between the first resistor R1 and the second resistor R2 floats up to V_{source}. But, since the first transistor Q1 is switched off, the second transistor Q2 is unable to receive bias current to remain switched

on (in conduction). As a result, the output voltage V_{output} rises equal to the voltage source V_{source}.

If the first wire loop LOOP A is shorted to the ground layer G, then the output voltage V_{output} goes high by equaling the voltage source V_{source}. Generally, this would result because of the following. The first transistor emitter $Q1_e$ is brought to ground because the node between the first resistor R1 and the second resistor R2 is brought to ground. This prevents current from flowing through the first transistor Q1. Thus, the first transistor Q1 is switched off. This in turn switches off the second transistor Q2 and the output voltage V_{output} rises equal to the voltage source V_{source}.

If the second wire loop LOOP B is shorted to the ground layer G, then the output voltage V_{output} goes high by equaling the voltage source V_{source}. Generally, this would result because of the following. Although the the node between the second resistor R2 and the third resistor R3 is brought to ground, a voltage still exists across the second resistor R2. However, since the first transistor base $Q1_b$ and the first transistor collector $Q2_c$ are both low, at or near zero volts, the second transistor Q2 is not allowed to turn on. Those skilled in the art will recognize that care should be taken to ensure the voltage rise across the loop circuitry cannot rise to 0.7 volts or more to allow it to turn on. This can be accomplished with a low impedance flex circuit trace and/or running minimal current through the loop circuit. With the second transistor Q2 switched off, the output voltage V_{output} rises equal to the voltage source V_{source}.

It should now be understood that under normal conditions the output voltage V_{output} is held low while during an attack the output voltage V_{output} goes high. Therefore, if the protected circuit 20 monitors the output voltage V_{output}, then the protected circuit 20 can determine when to initiate an appropriate response by watching for this change in output.

A particular arrangement for sizing the discrete components described above is setting the series resistors R1, R2 and R3 equal to 400k ohms, the forth resistor R4 equal to 100k ohms and insuring that the first and second loops do not exceed about 60 ohms each in their impedance. However, those skilled in the art will recognize that other arrangements may be better suited

to different types of applications.

Based on the above description and the associated drawings, it should now be apparent that the present invention improves many aspects of obtaining reliable and cost-effective protection of integrated circuits. Those skilled in the art will recognize that various modifications and adaptations can be made without departing from the spirit of the present invention. For example, other detection circuits operative with the trigger circuit may be employed. In particular, to achieve more power conservation, a field effect transistor FET may be used in place of the first transistor Q1. However, as described in the most preferred embodiment, the present invention seeks a simple cost effective yet robust arrangement. Therefore, the inventive concept in its broader aspects is not limited to the specific details of the preferred embodiments described above, but is defined by the appended claims and their equivalents.

What is Claimed is:

1. A tamper detection system for securing a protected integrated circuit from attack, the tamper detection system comprising:

a power source;

a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor, the first wire loop and the second wire loop being electrically isolated from each other but in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit; and

a detection circuit being in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop, then the detection circuit outputs a predetermined signal at a designated node.

2. The tamper detection system of claim 1, further comprising:

a ground layer in physical proximity to the first wire loop or the second wire loop; and

wherein if the first wire loop or the second wire loop are shorted to the ground layer, then the detection circuit outputs the predetermined signal.

3. The tamper detection system of claim 2, wherein:

the detection circuit includes a first transistor and a second transistor,

the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage cross the second resistor, the second transistor is operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

4. The tamper detection system of claim 3, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

5. The tamper detection system of claim 4, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

6. The tamper detection system of claim 1, wherein:

the detection circuit includes a first transistor and a second transistor, the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage cross the second resistor, the second transistor is

operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

7. The tamper detection system of claim 6, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

8. The tamper detection system of claim 7, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

9. A method of producing a tamper detection system for securing a protected integrated circuit from attack, the method comprising the step(s) of:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending

between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit; and

providing a detection circuit in operative communication with the trigger circuit and the protected integrated circuit, the detection circuit monitoring a flow of current through the trigger circuit, wherein if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop, then the detection circuit outputs a predetermined signal at a designated node.

10. The method of claim 9, further comprising the step(s) of:

providing a ground layer in physical proximity to the first wire loop or the second wire loop; and

wherein if the first wire loop or the second wire loop are shorted to the ground layer, then the detection circuit outputs the predetermined signal.

11. The method of claim 10, wherein:

the detection circuit includes a first transistor and a second transistor, the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage across the second resistor, the second transistor is operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

12. The method of claim 11, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor bias node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

13. The method of claim 12, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

14. The method of claim 9, wherein:

the detection circuit includes a first transistor and a second transistor, the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage across the second resistor, the second transistor is operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

15. The method of claim 14, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

16. The method of claim 15, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

17. A method of detecting an attempt to tamper with a protected integrated circuit, the method comprising the step(s) of:

providing a power source;

providing a trigger circuit including a plurality of resistors and a plurality of wire loops, the plurality of resistors including a first resistor, a second resistor and a third resistor, all of which being wired together in series and operatively connected to the power source, the plurality of wire loops including a first wire loop extending between the first resistor and the second resistor and a second wire loop extending between the second resistor and the third resistor;

keeping the first wire loop and the second wire loop electrically isolated from each other;

placing the first wire loop and the second wire loop in physical proximity to each other so as to form a protective mesh that envelopes the protected integrated circuit;

providing a detection circuit in operative communication with the trigger

circuit and the protected integrated circuit, the detection circuit monitoring a flow of current through the trigger circuit; and

if the flow of current through the trigger circuit is altered because of an open condition in the first wire loop or the second wire loop or a short between the first wire loop and the second wire loop, then outputting a predetermined signal at a designated node of the detection circuit.

18. The method of claim 17, further comprising the step(s) of:

providing a ground layer in physical proximity to the first wire loop or the second wire loop; and

if the first wire loop or the second wire loop are shorted to the ground layer, then outputting the predetermined signal.

19. The method of claim 18, wherein:

the detection circuit includes a first transistor and a second transistor, the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage across the second resistor, the second transistor is operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

20. The method of claim 19, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base

node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

21. The method of claim 20, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

22. The method of claim 17, wherein:

the detection circuit includes a first transistor and a second transistor, the first transistor is operatively connected across the second resistor so that the first transistor is allowed to develop a bias voltage across the second resistor, the second transistor is operatively connected across the first transistor and ground so that the second transistor is activated by an output current received from the first transistor, and the designated node is located between the power source and the second transistor.

23. The method of claim 22, wherein:

the detection circuit further includes a forth resistor connected between the power source and the second transistor;

the first transistor is a PNP type having an emitter node, a base node and a collector node, the first transistor emitter node is connected between the first resistor and the second resistor, the first transistor base node is connected between the second resistor and the third resistor;

the second transistor is a NPN type having an emitter node, a base node and a collector node, the second transistor base node is connected to the first transistor collector node, the second transistor emitter node is connected to ground, the second transistor collector

node is connected to the forth resistor; and

the designated node is between the forth resistor and the second transistor collector node.

24. The method of claim 23, wherein:

the predetermined signal is a high voltage condition substantially equal to the power source.

TAMPER DETECTION SYSTEM FOR SECURING DATA

Abstract of the Invention

A tamper detection system includes a trigger mechanism system and a detection circuit that operate in combination to protect an integrated circuit from attack. The detection circuit connects to the trigger mechanism system that is basically a protective mesh that consists of two separate loops of wire held in close proximity to each other and an optional ground layer. The mesh is such that an attempted penetration is highly likely to cause an open of either loop or a short of one loop to the other. The detection system recognizes shorts and opens in the mesh. The detection circuit is intended to be very simple in its operation it that it does not require a sophisticated stimulus and response set to operate. It is designed to be polled on a regular basis for indications of a change in its operation.

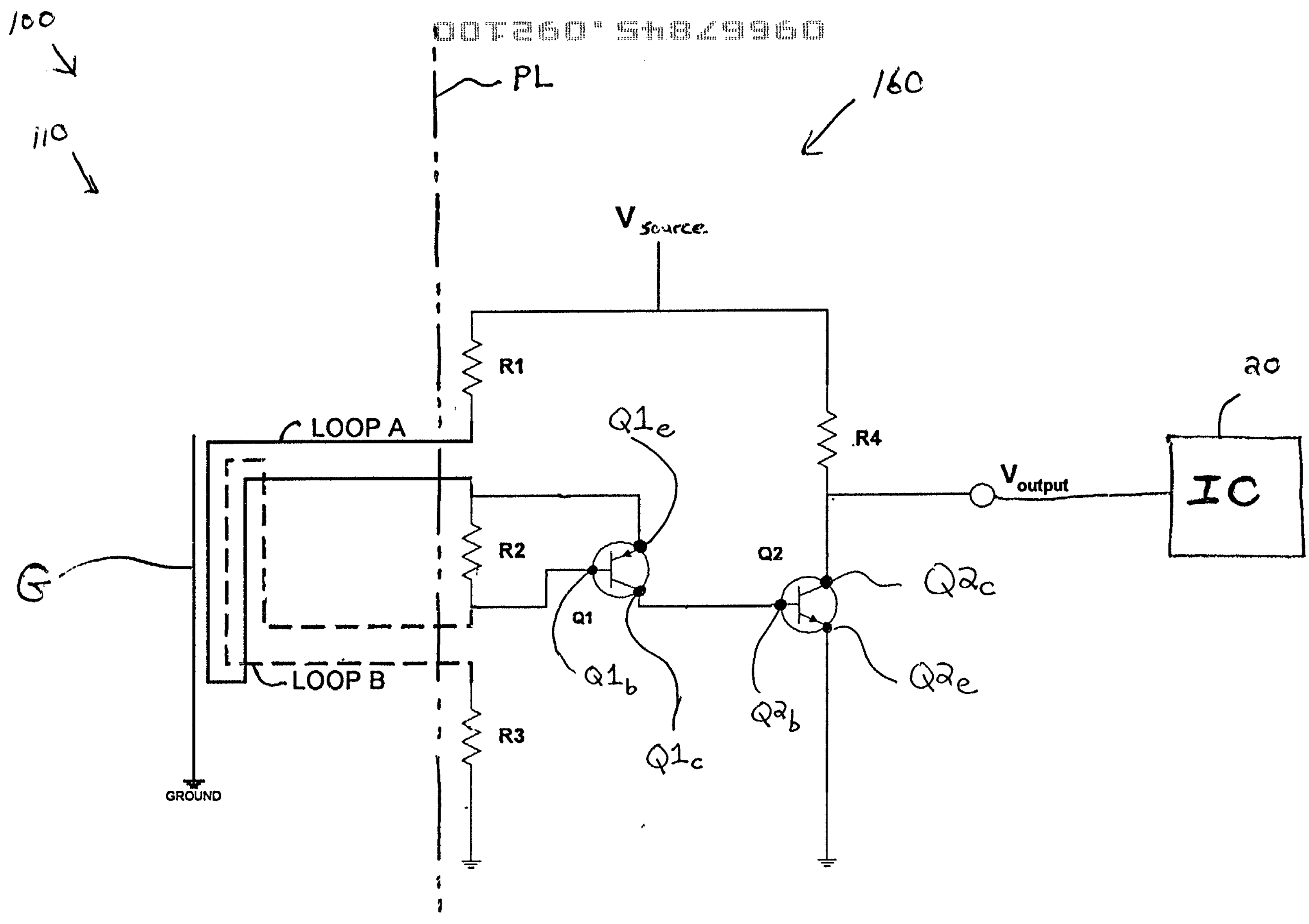

FIGURE 1

F-208
1-2

F-208
2-2

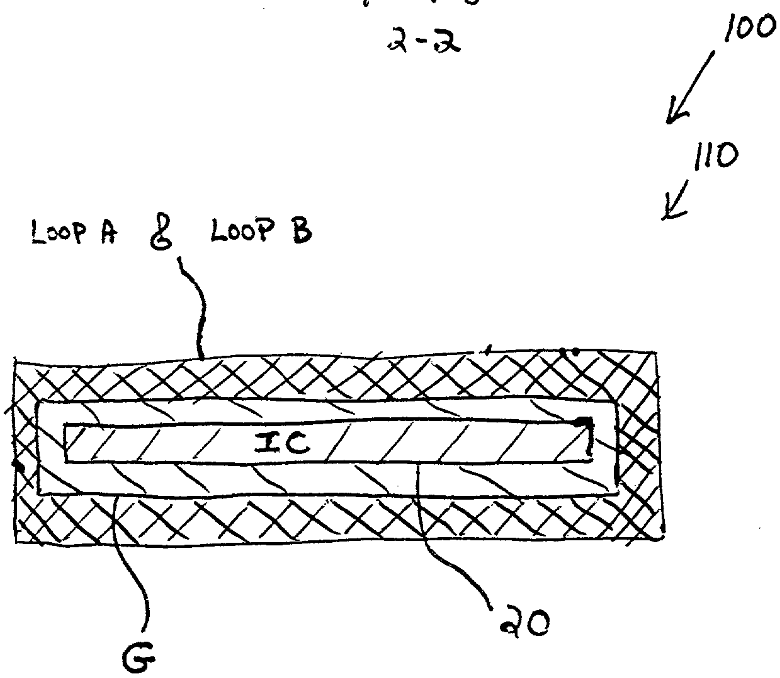

Fig. 2

Express Mail label number is EE628583118US.

DECLARATION AND POWER OF ATTORNEY Patent Application	Attorney's Docket Number F-208

As below named inventor, I hereby declare that:

my residence, post office address and citizenship are as stated below next to my name;

I believe that I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled

TAMPER DETECTION SYSTEM FOR SECURING DATA

described and claimed in the attached specification;

I have reviewed and understand the contents of the above-identified specification, including the claims;

I acknowledge my duty to disclose to the Patent and Trademark Office all information known to me to be material to the patentability of this application as defined in Title 37, Code of Federal Regulations, section 1.56; and

I do not know and do not believe the invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the invention was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months prior to this application, and that no application for patent or inventor's certificate on this invention has been filed in any country foreign to the United States of America prior to this application by me or my legal representatives or assigns.

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith;

Angelo N. Chaclas	Reg. No. 39,134
Michael E. Melton	Reg. No. 32,276
David E. Pitchenik	Reg. No. 24,020
Robert E. Meyer	Reg. No. 26,307

DECLARATION AND POWER OF ATTORNEY Patent Application	Attorney's Docket Number F-208
	Page 2 of 2

Address all telephone calls to Angelo N. Chaclas
at telephone No.: (203) 924-3844.

Address all correspondence to:

Angelo N. Chaclas
Pitney Bowes Inc.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name	Last Clark	First Douglas		Middle A.
Residence & Citizenship	City Wallingford		State CT	Citizenship USA
Post Office Address	Street Address 8 Laurelwood Drive	City Wallingford	State CT	Zip Code 06492

Signature of Inventor	**Date**
Douglas A. Clark	9-21-00